情 報 保 護 學 會 誌
第 13 券 第 2 號, 2003. 4

보안도구에 대한 우회공격 기법 분류 및 분석

손 태 식*, 서 정 우*, 구 원 본*, 민 동 옥*, 문 종 섭*, 박 현 미**, 이 병 권**

요 약

IDS, Firewall 등의 보안도구들은 보편화되어 있는 보안 솔루션이다. 시스템의 보안을 책임지는 이러한 도구들이 보안상 문제점(즉, 우회공격 가능성)을 가지고 있다는 것은 보안에 있어 근본적인 부분이 취약성을 내포하고 있는 것과 같다. 그러므로 시스템 및 네트워크에 대한 새로운 보안기법을 연구하기에 앞서 현재의 보안 솔루션들이 가지고 있는 우회공격과 같은 위험성을 해결하는 것 필수적이다. 따라서 본 논문에서는 일반적으로 사용되는 보안 솔루션들에 대한 우회공격 기술 분석 및 대응 방안에 관한 연구를 수행한다.

Ⅰ. 서 론

정보화의 역기능과 함께 현재 심각한 사회문제로서 대두되고 있는 크래킹과(일반적으로 해킹이라 불림) 같은 시스템 및 네트워크에 대한 불법적인 침해 문제의 대응방안으로서 Firewall, IDS 같은 보안 도구가 개발되었다. 현재 이러한 Firewall과 IDS는 대다수의 기업, 기관에서 설치되어 사용되고 있으며, 실제로 2005년까지의 전 세계적 시장 규모는 약 40억 달러로서 보안 서비스를 제외한 전체 보안 도구 시장의 1/4정도를 차지할 만큼 큰 비중을 차지하고 있는 대표적인 정보보호 솔루션이라고 말할 수 있다. 하지만 이렇게 Firewall과 IDS가 일반적인 정보보호 솔루션으로서 대다수의 네트워크 및 시스템의 보안을 책임지고 있다보니 이러한 보안 도구를 우회하여 공격할 수 있는 여러 우회 기법들이 현재 문제점으로 대두되고 있다. 앞서 서술한 것과 같이 Firewall 및 IDS는 가장 일반적으로 보편화되어 있는 보안 솔루션으로서, 관련된 해당 시스템 및 네트워크의 보안을 책임지는 이러한 도구들이 보안상 문제점을 가지고 있다는 것은 곧 정보보호에 있어 가장 근본적인 부분이 취약성을 내포하고 있는 것과 같다. 그러므로 시스템 및 네트워크에 대한 새로운 정보보호 기법 및 기술을 연구하기에 앞서 현재의 정보보호 솔루션들이 가지고 있는 우회공격과 같은 위험성을 해결하는 것이 개인의 시스템 및 국가 기간 시스템과 네트워크의 정보보호를 위한 최우선 사항으로 진행되어야 한다.

따라서 본 연구에서 가장 일반적으로 사용되는 보안 솔루션인 Firewall, IDS 그리고 Router에 대한 우회공격 기술 분석 및 대응방안에 대한 연구를 수행하는 것이 필요하다[7]-[8].

본 논문은 다음과 같이 구성되어 있다. 제2장에서는 우회공격 기술 동향을 분석하며 제3장에서는 실제 우회공격 기법에 대하여 분석하고 제4장에서는 우회공격 대응방안을 그리고 마지막으로 본 논문의 결론 및 향후 연구 방향을 서술한다.

Ⅱ. 우회공격 기술 동향 분석

2.1 IDS에 관한 우회공격 기법 동향

IDS에 대한 우회공격은 현재 대부분의 IDS에서 사용하고 있는 스트링 패턴매칭 기법의 취약성을 이용하는 방법이 가장 일반적이며 또한 현재는 TCP/IP 상의 프로토콜 특성을 이용한 fragmentation 기법이나 Covert Channel 형성의 방법 등도 사용된

* 고려대학교 정보보호대학원, 정보보호기술연구센터({743zh2k, jsmoon}@korea.ac.kr)
** 한국정보보호진흥원(hmpark@kisa.or.kr)

다. 또한 IDS의 가용 자원을 고갈시켜 IDS의 정확한 공격 판단을 어렵게 만드는 DoS 공격도 널리 사용되고 있는 실정이다. 일반적으로 IDS들은 스트링 패턴매칭 기법으로 침입을 판단하기 때문에 IDS의 룰 데이터베이스에 정의되지 않은 침입에 대해서는 탐지할 수 없게 되는 것이 이러한 취약성이 IDS 우회 기법에 널리 사용되게 된다.[16]

2.2 방화벽에 대한 우회공격 기법 동향

방화벽은 방화벽 시스템이 네트워크 환경에 적용되어진 이후 지금까지 해킹에 대해서 비교적 안전하게 네트워크를 보호해 왔다. 그러나 현재 나와 있는 모든 방화벽이 보안에 있어 안전하다고 할 수는 없다. 게다가 설치되어있는 방화벽 대부분이 잘못 설정되어 있거나 관리가 제대로 이루어지지 않아서 해커들에게 무방비로 열려있다. 최적화되고 강력한 보안정책이 유지되는 방화벽은 뚫고 들어가기가 거의 불가능하다. 대부분의 해커들은 이러한 사실을 알고 있으며 이러한 방화벽의 뒤를 공격하기 위해 방화벽을 우회하거나, DoS 공격 등을 이용하여 방화벽을 무력화시킨다.

2.3 라우터에 대한 우회공격 기법 동향

Router는 특정 네트워크에서 다른 네트워크로 패킷을 전송하는 장비로 3계층에서 동작한다. Router의 고유한 기능은 이처럼 패킷 전송을 위한 라우팅에 있다. 하지만 최근 네트워크의 효율성 못지 않게 보안이 심각한 문제로 대두되면서 Router는 단순히 라우팅만을 위한 장비가 아니라 보안기능을 갖춘 장비로 발전되고 있다. 기관에서 Router에서 제공하는 이러한 보안기능에 대해 알고 적용함으로써 전체 기관의 보안을 한층 높일 수 있을 것이다. 특히, 이러한 많은 기능 중에서도 접근 제어 리스트의 취약성과 소스 라우팅 기능의 취약성 등으로 인해 현재 Router를 이용한 우회공격이 보고되고 있다. 따라서 Router 자체의 보안에도 많은 신경을 쓸 필요가 있다. 하지만, 많은 일선기관에서는 아직 Router의 보안기능을 충분히 활용하지 못하고 있는 것으로 보이며, 이로 인해 인터넷의 수많은 위협으로부터 내부 시스템들을 무방비 상태로 노출시키고 있는 현실이다.

Ⅲ. 보안도구 우회공격 기법 분석

3.1 보안도구 우회공격 기법 분류

본 절에서는 IDS, Firewall, Router등의 보안도구에 가능한 우회공격을 각 공격의 대표 특성에 의하여 분류한다. 현재 사용되는 대부분의 우회 도구 공격기법들은 대부분이 IDS에 초점을 두고 있지만, IDS 우회를 목적으로 하는 공격 도구일지라도 그 우회공격 도구에서 사용되는 우회 기법은 IDS가 가지는 패킷 필터링, TCP/IP 프로토콜 기반으로 작동 등의 특성에 의존적이므로 IDS, Firewall, Router 등 보안 도구에 따른 우회공격의 구분은 큰 의미가 없다. 또한 Covert Channel을 통한 우회공격기법은 어떤 보안 도구를 사용할지라도 생성되는 Covert Channel의 특성을 파악하지 못한다면 우회공격에 대해 특별한 대응방안을 마련하기 어렵다.

따라서 본 연구에서는 보안 도구에 따른 우회 기법의 분류, 분석이 아닌 현재 보고되고 있는 여러 보안 도구 우회 기법들 중 우회공격기법 자체의 특성에 따라 분류한 후 분류된 각 범주에 따라 세부 우회공격기법을 분석하였다. 본 연구에서의 우회공격기법 분류는 [1,5,7,12]와 같은 참고문헌의 Insertion, Evasion, DoS 분류를 바탕으로 TCP/IP 프로토콜 상의 특성에 따라 분류하는 것을 기본으로 하였으며, 그 외 보안 도구의 취약성이나 일반적인 사회공학기법을 이용한 기법 분류를 포함하였다.

이러한 우회공격기법의 분류는 첫 번째로 보안도구의 패킷 필터링, 스니퍼링 특성에 따른 분류, 두 번째로 TCP/IP 프로토콜에 기반한 분류, 세 번째로 보안도구 취약성에 의한 분류 그리고 사회 공학적 기법에 의한 분류로 크게 구분하였다. 이런 분류 항목은 다음의 [표 1], [표 2]에 자세히 나타나 있으며 또 각 세부 공격기법에 대한 공격 분류 인덱스를 통하여 추후 분석될 우회공격 도구들과의 연관성을 파악 할 수 있도록 하였다.

3.2 패킷 필터링 특성에 의한 공격기법 분석

3.2.1 Insertion 우회공격기법 분석

현재 대부분의 네트워크기반-IDS에서는 원시데이터의 수집과 이에 대한 프로토콜 분석을 수행하는 메커니즘을 가지고 있다. 이는 네트워크 트래픽의 관찰을 통해 의심 가는 패턴을 가진 행동들을 세심하게 구별하는 것으로, 정확한 패턴인식을 위해서는 원시데이터를 수집하는 device에 대한 의존성이 커질 수밖에 없는 문제점이 있다.

Insertion이란 IDS의 device에 의존적인 면과

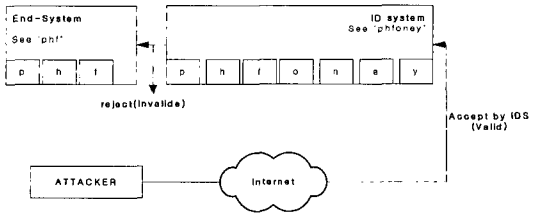
특정 취약점을 이용한 공격 종류로서, 공격자에 의해 생성된 정당하지 않은 패킷이 IDS에서 잘못 인지됨으로서 발생할 수 있는 공격이다. 이 공격의 정확한 탐지를 위해서는 일반적인 IDS들이 가지고 있는 공격 탐지방법의 문제점을 우선 고려하여야 한다. IDS는 네트워크 트래픽에서 특정 패턴을 가진 데이터를

〔표 1〕 우회공격 분류표

대 분 류	특성에 따른 항목	세부 공격기법			공 격 분 류
Packet Filtering, Sniffering 에 의한 분류	Insertion	Unicode	URL encoding	UTF8 encoding	FS-I-가
				HEXA encoding	
				Percent encoding	
				Unicode encoding	
				Double-eval encoding	
			etc	Self-Referencing Directories	FS-I-나
				Z Parameter hiding	
				Long URL	
				Multiple slashes	
				Reverse traversal	
		TCP/IP	FIN, RST spoofing	short TTL	FS-I-다
				TCP checksum validation	
			Data Spoofing		FS-I-라
	Evasion	String Matching Weakness	Method Matching		FS-E-가
			Session Splicing		
			Parameter Request Ending		
			Http Mis-formatting		
			Case Sensitivity		
			Null method processing		
		Session Assembly Weakness	Session Splicing		FS-E-나
			fragment	Tiny Fragment	FS-E-다
				Fragment Overlap	
				Fragment overwrite	
				Fragment time-outs	
	DoS	Resource Exhaustion	Smurf		FS-D-가
			Jolt2		
			Ping flooding		
			CPU hog		
			RPC locator		
			Bubonic		
			Ssping		
		Abusing Reactive IDS	land		FS-D-나
			ping of death		
			syn flood		
			icmp flood		
			winnuke		

〔표 1〕 우회공격 분류표(계속)

대 분 류	특성에 따른 공격 항목	세부 공격기법	공 격 분 류
TCP/IP 프로토콜 특성에 의한 분류	Network Layer	IP Insertion	TI-N-가
		MAC Address	
		IP Fragmentation	
		IP covert channe	
	Transport Layer	TCP Insertion	TI-T-가
		TCB De-Synchronization	
		TCP Stream Reassembly	
		TCB Teardown	
		TCP covert channel	
Vulnerability에 의한 분류	IDS	System configuration error - key encryption/key management	V-I-가
		Unicode/URL parcing error	V-I-나
		Denial of Service	V-I-다
	Firewall	System configuration error - key encryption/key management	V-F-가
		ACL control error	V-F-나
		Exceptional handling error - buffer overflow	V-F-다
	Router	System configuration error - key encryption/key management	V-R-가
		ACL control error	V-R-나
		Exceptional handling error - buffer overflow	V-R-다
Social Engineering 기법을 사용한 기법 분류	E-mail		SE-1-1
	Dumpster Diving		
	Office Snooping		
	Friendship		
	Trust		
	Time		



〔그림 1〕 Insertion 공격

찾기 위하여 패턴-매칭 알고리즘을 사용한다.

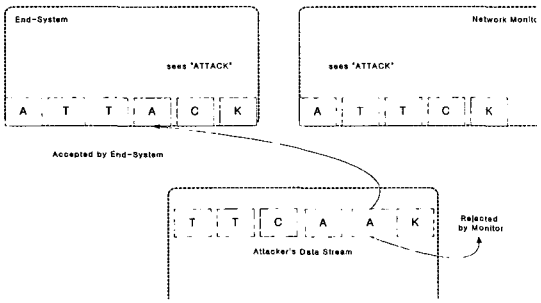
예를 들면, PHF-CGI공격을 탐지하기 위하여 HTTP request 패킷에서 "phf"문자열을 찾기 위한 알고리즘. 공격자가 이러한 방법에 대한 정보를 사전에 인지하고 있다고 가정한다면, "phf"가 아닌 "phfoney"와 같이 "oney"에 대한 문자열을 단순히 삽입함으로서 IDS를 우회할 수 있다. Insertion공격은 〔그림 1〕을 보면 더욱더 명확해진다. 공격자에 의해서 임의로 만들어진 패킷이 IDS에서는 정상으로 받아들여지고 마지막 end-system에서는 비정상적이라 판단, 패킷을 수용하지 않는 상황을 보여준다. 이와 같이 insertion공격은 IDS가 비교적 보호하고 있는 영역으로 향하는 패킷의 허용도가 심하지 않을 경우, 언제든지 가능하며, 현재 IDS에서 발견되었고, 발견될 가능성이 가장 높은 공격중 하나이다.

3.2.2 Evasion 우회공격기법 분석

네트워크 기반 IDS는 end-system에서 IDS가 reject한 패킷을 받아들인다. 판단이 잘못된 패킷들은 IDS에 빠르게 지나쳐버려 부당하게 이용될 수

있다. 이러한 패킷들을 "evading"된 패킷이라고 보통 말한다. 또한, evasion attack이라 부르기도 하는데, 이것은 부당하게 이용될 수 있고, IDS의 정확성을 매우 떨어뜨린다.

우회공격은 방법론적으로 Insertion attack과 유사하게 pattern matching을 피하게 만든다. Insertion attack은 공격자가 HTTP request를 보낼 시, 첨가된 data를 통해 IDS 판단시 해가 없는 걸로 착각하게 만드는데 반해, [그림 2]와 같은 Evasion 공격은 공격자가 패킷에 같은 요청을 분할하여 보냄으로서, IDS가 잘못된 판단을 내리게 하고, 스트림 데이터의 한 부분을 제거함으로서 IDS가 잘못된 패킷을 인정하게끔 한다.



[그림 2] Evasion 공격 개요

보안도구에 대한 Evasion 공격은 스트링 패턴 매칭 기법을 주로 사용하는 IDS에 적용될 수 있는 Method Matching, Parameter Request Ending, Http Mis-formatting, Case Sensitivity, Null method processing, Unicode Bypassing vulnerability등의 String Matching 취약성과 일반적인 보안도구 모두에 적용될 수 있는 Session splicing, 다양한 Fragmentation공격 등의 Session Assembly 취약성으로 분류 할 수 있다.

3.2.3 DoS 공격기법 분석

시스템 정지 및 재시동 을 유도하는 방식은 보통의 경우 에러나 디바이스 간의 충돌 등이 발생할 때 나타난다. 이러한 방식은 Window 환경에서 네트워크 디바이스를 무기한 대기 상태로 유도하는 기법, 접속되지 않거나 접속되어 지지 않았었던 IP 주소 등을 이용한 부적절한 DNS 명령을 수행하게 하는 기법 등이 있으며 공격법에는 Ping of Death, SYN Flood, Land 등이 있다. 이상의 방법은 IDS 시스템의 Reconfiguration을 유도함으로써 재부팅 되는 동안 혹은 재설정 되는 동안의 시간을 이용하여 공격을 감행하는 시나리오가 예상된다. 또한 사용이 요구되는 모든 자원의 완전 소모를 유도하는 방식은 메모리 고갈, 디스크 채우기, 프로세스 만들기, Bandwidth Overload 등이 있으며 이에 해당하는 공격법에는 Ping Flooding과 위에서 언급했던 ICMP의 악의적 사용법에 하나인 Smurf 등이 있다. 이 방법은 네트워크 기반의 IDS 의 경우 네트워크의 Bandwidth의 과부하를 유도하여 IDS의 성능 저하 및 작동 정지 상황을 유도하는 방식이다. 호스트 기반의 IDS 의 경우에도 시스템 자체의 부하 적재(CPU, Process, Disk space, Bandwidth)를 이용한 성능 저하 및 기능 정지를 유도하기 때문에 이를 이용한 혹은 네트워크 기반의 공격과 호스트 기반의 공격의 결합 공격을 유도하는 등 다양한 형태의 공격이 가능하다.

3.3 TCP/IP 특성에 의한 공격기법 분석

3.3.1 IP layer 우회공격기법 분석 - IP Insertion

공격자가 IDS의 허용을 받는 IP 패킷을 보내는 방법은 많이 있다. 즉, 공격자에 의해서 임의로 만들어진 패킷이 IDS에서는 정상으로 받아들여지고 end-system에서는 비정상이라고 판단하여 패킷을 수용하지 않을 수 있다. 그러므로 end-system의 운영체제와 IDS에서 패킷을 수용하지 않는 조건이 일치해야 한다. 만일 운영체제와 IDS간에 일치가 되지 않는다면, 이 IDS는 insertion 또는 evasion 공격 등에 취약점을 갖게 된다.

(1) 잘못된 헤더 옵션 설정(TTL)을 이용한 우회

수신측이 IP 데이터그램을 버리도록 하는 가장 쉬운 방법은 IP 데이터그램에 잘못된 헤더 필드를 갖게 하는 것이다. IP 패킷의 헤더 필드는 RFC 731[7]에 설명되어 있다. 잘못된 헤더 필드를 만드는 방법 중 하나는 TTL 필드를 사용하는 것이다. IP 패킷의 TTL(time to live) 필드는 패킷이 수신측까지 도착하는데 거칠 수 있는 hop들의 수를 나타낸다. 그리고, 항상 라우터는 패킷을 받아 보내면서 TTL을 1씩 줄인다. TTL이 0이 되면, 해당 패킷은 라우터에 의해 버려진다. 만일 IDS가 보호하려는 end-system과 네트워크상의 위상이 다른 경우, 공격자는 IDS에 도착하기에는 충분하지만 end-system까지는 도달할 수 없도록 TTL을 설정

하여 공격할 수 있다.

(2) DF 옵션을 이용한 우회(MTU)

다른 방법 중 하나는 IP 헤더의 "Don't Fragment"(DF) 플래그를 이용하는 것이다. 만일 목적지 시스템으로 전송하여야 할 패킷의 크기가 네트워크 상에서 수용가능하지 않을 경우, 패킷을 수용이 가능하도록 분할해주어야 한다. 그러나, DF 플래그가 설정되어 있으면 패킷의 크기가 네트워크 대역폭보다 큰 경우 분할하지 않고 간단히 버린다. 만일 IDS 네트워크의 최대 패킷 사이즈(MTU : maximun packet size)가 수신 시스템의 최대 패킷 사이즈보다 큰 경우, 공격자는 수신 네트워크의 최대 패킷 사이즈 보다 크게 사이즈를 설정하고 DF 비트를 설정하여, IDS에서는 패킷을 확인 가능하지만 end-system에는 도달하지 못하도록 하여 공격할 수 있다.

(3) IP Option을 조작하여 우회

"time-stamp" 옵션을 처리하는 코드는 잘못된 옵션을 갖은 패킷을 버릴 수도 있다. time-stamp는 해당 패킷이 유효한지를 나타낸다. IDS가 모든 패킷의 time-stamp를 일일이 확인하지는 않으므로, 공격자는 임의로 time-stamp를 조작하여 IDS에서는 정상 처리되지만 end-system에는 수용되지 않도록 하여 공격할 수 있다. "checksum" 옵션의 경우도 마찬가지로end-system에서는 checksum이 틀린 패킷을 버릴 것이다. 그러므로, IDS가 모든 패킷의 checksum를 일일이 확인하지는 않는다면, 이 IDS는 Insertion 또는 evasion 공격에 취약점을 갖게 된다.

3.3.2 IP layer 우회공격기법 분석 - MAC address

insertion 공격에 의한 문제는 link-layer addressing 때문에 존재할 수 있다. 네트워크 모니터와 같은 LAN상에 있는 공격자는 IDS의 link-layer 프레임에 직접 연결할 수 있다. 만일 공격자가 IDS의 링크-레이어 주소를 알고 있다면, 공격자는 IDS로 가짜 패킷을 손쉽게 보낼 수 있다. IDS가 수신 받은 패킷의 MAC 주소를 확인하지 않는다면 LAN상의 다른 시스템들은 그 패킷을 처리하지 못할 수 있다. 공격자가 네트워크 모니터의 링크-레이어주소를 알지 못한다 하여도, 네트워크 모니터가 가짜 주소로 설정된 프레임에 의해 오작동 하도록 할 수 있다. 즉, 만일 IDS가 올바른 링크-레이어 주소의 IP 헤더에 수신지 주소를 확인하지 않는다면, 주소가 잘못 설정된 링크-레이어 프레임으로 판단할 수 있다.

3.3.3 IP layer 우회공격기법 분석 -IP 은닉 채널

은닉채널이란 시스템 보안 정책을 위반하는 어떤 방법을 사용하여 정보를 전송하는 프로세스에 의해 이용될 수 있는 임의의 통신 채널로서 정의된다. 근본적으로 이와 같은 통신 채널은 일반적인 컴퓨터 설계상의 통신 수단이 아니며 보통 특정 정보에 접근하는 것이 허락되지 않는 프로세스나 사용자들에게 정보를 전송하기 위한 수단으로서 사용될 수 있다.

이러한 TCP/IP 은닉채널은 실제로 IP 패킷의 Identification field를 이용하는 방법, IP 패킷의 checksum field를 이용하는 방법, TCP initial sequence number field를 이용하는 방법, TCP acknowledge sequence number field를 이용하는 방법, 패킷의 타이밍 정보를 이용하는 방법 등 여러 방법들이 존재한다.

3.3.4 TCP layer 우회공격기법 분석 - TCP Insertion

IP 프로토콜과 같이, TCP에서 패킷을 삽입하는 다른 몇몇 방법들이 존재한다. 그러나 TCP에서의 처리는 복잡하므로, 수신된 패킷을 버리는 경우의 조건이 많이 있다. 그러므로, IDS가 수신 시스템과 같은 방식으로 TCP 패킷들을 처리하지 않는다면, insertion 공격에 취약점을 가지고 있는 것이다.

TCP 패킷으로부터 데이터를 뽑아내고 헤더 필드 부분을 확인하지 않고 재조립하게 된다. 이는 TCP 세션 모니터를 패킷 insertion 공격에 취약하게 만든다. 그러므로, TCP 패킷의 데이터를 확인하기 전에 헤더 필드를 확인해보는 것이 중요하다. 필드에서 확인하기 가장 쉬운 부분이 "CODE" 이다. 이것은 TCP 세그먼트의 메시지에 종류를 결정하는 것이다. TCP 코드는 이진 플래그의 순열로 되어 있는데, 이 플래그가 잘못 조합되어 있는 경우 해당 패킷은 버려져야 한다.

잘못된 헤더 옵션 설정(ACK 부재)을 이용한 우회공격은 많은 TCP 구현에서 "ACK" 플래그가 설정되어 있지 않은 패킷의 데이터를 허용하지 않는 것을 이용한다. 그러나, TCP 상황에 따라서, TCP 구현에서는 SYN 패킷에 데이터를 허용해야할 필요가 있다. 이는 매우 난해하고 불분명하므로, 많은 구현들에서는 이 문제를 올바르게 다루지 않고 있

다. 만일 IDS가 SYN 패킷의 데이터를 고려하지 않는다면, evasion 공격에 취약점을 갖게 된다. 또한 inserion 공격에도 취약점을 갖는 것이다.

TCP Option을 조작하여 우회하는 기법은 IP에서와 같이, IDS는 TCP 옵션들을 정확하게 처리해야 한다. 불행히도, TCP 옵션의 처리는 IP 옵션의 처리보다 더 어렵다. 첫 번째 원인은, 몇몇의 TCP 옵션들은 최근에 새로 만들어졌기 때문이다. 예를 들어, timestamp, window scale등이 있다. 다른 원인은 연결의 상태에 따라 TCP 옵션에 대한 규정이 결정된다는 것이다. 즉, 어떤 옵션들은 어떠한 연결 상태에서는 잘못 된 것이라는 것이다. RFC1323에서는 신뢰도를 증가시키고 고속의 통신 환경에서 TCP 수행을 위한 두 개의 새로운 TCP 옵션을 소개하고 있다. RFC1323에는 만일 옵션이 미리 약속되어 있다면 non-SYN 세그먼트의 경우들을 설명하고 있다.

3.3.5 TCP layer 우회공격기법 분석 - TCP reassembly

불안정한 네트워크에서는 TCP 패킷이 항상 정상적으로 전송된다는 보장이 없다. 타임아웃에 의해서 재전송을 하거나, 혹은 순서가 바뀌어서 패킷이 도착하고, 패킷이 겹치는 경우도 있다. 이런 경우, IDS에서 침입을 탐지하지 못하거나 잘못된 침입 탐지를 할 수 있다. 그러므로 TCP 프로토콜에 맞게 이 패킷들을 reassembly 하지 않으면 TCP 상위에서 수행되는 침입탐지는 정확하다고 볼 수 없다.

Basic Reassembly Problem은 만약, IDS가 시퀀스 넘버를 사용하지 않고, 패킷이 들어오는 순서대로 reassembly 할 때 공격자가 고의적으로 순서를 바꾸어서 공격 패킷을 보내면 IDS는 이를 탐지할 수 없다. 이러한 IDS는 정상적인 TCP 패킷이 순서가 섞여서 들어왔을 때에도 IDS 자체가 시퀀스 넘버를 사용하지 않으므로 false positive alert을 할 수가 있다.

Challenges To Reassembly은 시퀀스 넘버를 검사하는 IDS에서 목적지 시스템의 윈도우(버퍼에 들어올 수 있는 데이터를 표현)를 확인하는 시간이 목적지 시스템에 있는 윈도우가 변화하고 반응하는 시간과 어긋난다면, 시간을 주기로 계속 도착하는 패킷들을 IDS가 정확히 검사 할 수 없다. 이런 IDS들은 잠재적으로 삽입공격에 취약해 진다. 공격자가 동일한 시퀀스 넘버를 갖고, checksum만 다른 여러개의 데이터를 보내게 되면, IDS가 패킷의 정당성을 결정할 만한 충분한 자료가 없기 때문에 패킷을 통과시키게 된다. IDS가 통과시킨 한 개의 패킷이 목적지 시스템에 도착하여 공격이 가능해 진다. 공격자는 IDS에 정당한 패킷과 목적지 시스템에 도착하지 못할 패킷을 보내서 IDS가 받아들이는 패킷들을 결정한다. 전형적인 삽입공격이며, 잠재적으로 IDS와 실제연결의 동기화를 해제시킨다.

Overlap은 TCP도 IP fragment처럼 다양한 크기와 순서로 도착할 수 있다. IP fragmentation의 Overlap 공격과 마찬가지로 TCP도 데이터 위에 새로운 데이터를 겹쳐 씀으로써 공격패킷을 만들 수 있다. TCP 세그먼트들의 Overlap 규칙은 IP 데이터그램의 Overlap 규칙과 아주 흡사하다. TCP 세그먼트의 Overlap 공격을 할 때, 공격자는 하나의 겹쳐쓴 하나의 세그먼트를 수반하거나 혹은 세그먼트 하나만 보내서 IDS 필터링에 걸릴만한 문자열이 없도록 패킷을 생성할 수 있다. 공격자가 생성한 패킷이 IDS를 통과하게 되면, 목적지 시스템에서 패킷스트림이 겹쳐씌여 지면서 공격이 가능하게 된다.

3.3.6 TCP 우회공격기법 분석 - TCP Desynchronization

Post Connection SYN은 TCP 시퀀스 넘버를 사용하여 IDS를 우회하는 기법으로서, IDS가 기존의 동기화를 해제하고, 공격자가 설정한 SYN 패킷에 의해 새롭게 동기화를 시키는 것이 목적이다. 우선, 정상적인 연결설정을 확립한 후에 순서에 맞지 않는 시퀀스 넘버를 갖는 SYN 패킷을 데이터 스트림 속에 넣어서 목적지 시스템으로 보낸다. 목적지 시스템은 시퀀스 넘버가 맞지 않으므로 이 SYN 패킷을 무시하게 되고, IDS는 이 SYN 패킷에 의해 새롭게 동기화가 된다. IDS가 새롭게 동기화 하게 되면 기존에 있던 연결은 IDS와 동기화가 해제되었기 때문에 IDS를 피할 수 있다. 그리고, SYN 패킷에 의해서 IDS를 재동기화 하는 것을 성공했다면, IDS를 재동기화 했던 시퀀스 넘버를 가진 RST 패킷을 보내어 재동기화된 연결을 끝낸다.

Pre Connection SYN는 이 기법은, 실제 연결이 이루어지기 이전에 비정상적인 TCP checksum을 가진 초기화 SYN을 보내서 IDS를 동기화 시키는 것이 목적이다. IDS가 SYN의 서브시퀀스를 무시할 정도로 지능적이지만, TCP checksum을 확인할 정도는 아니라면, 이 공격은 실제 연결이 이루어지기 전에 공격자가 위조한 SYN 패킷에 의해 IDS가 동기화 된다. 공격자는 checksum을 조작

하여 목적지 시스템은 받아들이지 않고, IDS는 받아들이는 SYN 패킷을 만들어서 실제 연결이 이루어지기 전에 보낸다. IDS는 이 SYN 패킷에 의해 동기화 되고, 목적지 시스템에 실제적인 연결은 이루어지지 않는다. 다시 실제연결을 이루기 위한 SYN 패킷을 목적지 시스템에 보내게 된다. 이 때 IDS는 이미 동기화 되어있는 상태에서 새로운 SYN을 받게 되므로 이것을 무시하게되고 목적지 시스템은 이 SYN 패킷에 의해 연결이 성립되게 된다.

3.3.7 TCP 우회공격기법 분석 - TCP 은닉 채널

IDS와 같은 보안도구들은 TCP/IP 프로토콜의 처리 과정에 있어 insertion이나 evasion과 같은 공격에 취약성을 가질 수 있으며 또한 하위 레이어 프로토콜에서 발생하는 우회공격에 대한 취약성들은 상위 레이어의 프로토콜에도 영향을 주게 된다. 또한 IDS에 탐지되는 많은 공격들은 TCP 연결이 확립된 후에 일반적으로 이루어지게 된다. 그러므로 IDS가 TCP 연결에 대해서 연결 과정을 확인하고 연결된 데이터들에 대해서 대상 시스템의 재조립 과정 전에 패킷들을 재조립하여 공격 여부에 대하여 탐지하는 것이 필요하며 이러한 IDS의 TCP 모니터링에 대한 기능미비를 이용한 우회공격들이 발생할 수 있다.

3.4 보안도구 취약성에 의한 공격기법 분석

IDS, Firewall, Router 등은 일반적인 정보보호 솔루션으로써 대다수의 네트워크 및 시스템의 보안을 책임지고 있다. 하지만 이러한 보안 도구를 우회하여 공격할 수 있는 여러 우회 기법들이 현재 문제점으로 대두되고 있다. 특히 이러한 보안도구에 대한 우회공격은 일차적으로 해당 시스템 및 네트워크를 관리하는 관리자의 관리 부족이 근본적인 원인을 제공하고 있으며, 또한 보안도구의 잘못된 정책설정에 의한 우회공격, IP fragmentation과 같은 통신 프로톨콜의 취약성을 이용하는 우회공격, 침입탐지 시스템의 오류 판정을 이용한 우회공격 그리고 보안도구 자체의 오류를 이용하는 우회공격 등이 널리 사용되고 있다.

3.4.1 IDS 취약점 분석 - %u 인코딩에 의한 IDS 우회 취약점

침입탐지 시스템은 UTF와 hex 인코딩 요청에 대하여 HTTP 인코딩과 같이 여러 가지 형식들을 디코드하는 것이 가능해야한다. 대부분의 IDS벤더들의 제품들과 프리웨어 IDS제품들은 UTF나 hex 인코드 요청에 의한 공격 문자열들을 분석할 수 있는 기능을 가지고 있다. URL 인코딩을 위한 두 가지 주된 방식은 UTF(%xx%xx) 또는 hex(%xx)로 인코딩하는 것이다. 여기서 xx는 적적한 hex 값을 나타낸다. 마이크로 소프트 IIS 웹 서버는 인코딩을 위한 두 가지의 타입을 포함하고 있다. 하지만 HTTP 표준 방식이 아닌 다른 인코딩 방식으로 처리하고 있다. 그 결과 대부분의 침입탐지시스템(IDS) 시스템들이 다른 방식으로 구현된 인코딩을 인식하지 못하고 디코딩을 수행하지 못하게 된다. %u 인코딩의 목적은 유니코드 문자 스트링 표현이 가능하다는 것이다. 하지만 %u 인코딩은 표준방식이 아니기 때문에 침입탐지시스템(IDS)은 %u 문자열을 디코딩 하지 않는다. 그결과, %u 문자열을 이용한 공격을 탐지하는 기능을 갖추지 않은 침입탐지시스템(IDS)의 IIS 웹서버는 스캔 및 공격을 받는다. 이외에도 기형적인 IP 패킷에 의한 DoS 공격 취약점 및 IDS에 설치된 ISS RealSecure의 기본적인 키 관리 취약점 등이 존재한다.

3.4.2 Firewall 취약점 분석 - HTTP 프락시 요청에대한 취약점

내부 또는 외부 클라이언트가 프락시와 같이 이웃한 인터페이스(방화벽 인터페이스)를 사용하기 위하여 구성되어 있을 때, 공격대상 호스트의 내부 포트들을 이용하여 엑세스가 가능하다. 이외에도 Gauntlet Firewall 버퍼 오버플로우 취약점 및 Network Associates Gauntlet Firewall Denial of Service 공격 그리고 Axent Raptor Firewall에서의 Denial of Service 취약점 등이 존재한다.

3.4.3 Router 취약점 분석 - 패킷 사이즈가 큰 ICMP ECHO 전송에 의한 Denial of service 공격

CBOS(Cisco Broadband Operating System) 버전 2.3.8과 이전의 버전을 실행하고 있는 Cisco 600 시리즈 라우터 제품들은 버퍼 오버플로우에 대한 Denial of service에 대한 공격에 취약점을 가지고 있다. 65,600 바이트 크기 또는 그 이상의 크기를 갖는 ICMP ECHO (ping) 패킷을 라우터에 전송함으로써, 공격자는 내부 변수를 오버플로우 시키거나 라우터를 다운시킨다. 이와 비슷한 공격으로

써 라우터에 TCP SYN 패킷들을 계속적으로 보냄으로서 시스템이 모든 가능한 TCP 소켓들을 모두 소비하도록 하는 공격도 있는데, 그 결과 라우터에 새로운 TCP 세션을 완전하게 할당할 수 없다. SYN Denial-of-Service 공격과의 차이점은 매초당 한번씩 패킷들을 흘려 보낸다는 차이점이 있다. 이공격을 받은 Cisco 600 시리즈 라우터는 정상적인 기능을 수행하기 위하여 시스템을 다시 시작해야 한다. 이외에도 Linksys EtherFast BEFVP41 케이블/DSL VPN Router 키 암호화에 대한 문제점 및 3Com OfficeConnect HTTP Denial of Service 그리고 패스트/기가바이트 이더넷 카드를 사용하는 시스코 기가바이트 스위치 Router에 대한 ACL 우회 및 DoS 취약점등이 존재한다.

3.5 사회공학기법에 의한 공격기법 분석

사회공학이란 신뢰할 수 없는 사람이 한 회사의 보안 담당자에게 보안을 허술하게 하도록 설득 또는 유도하는 방법 등을 말한다. 고객지원팀이라고 확인되지 않은 통화자가 고객지원팀을 사칭하여 고객의 패스워드를 요구하는 것은 사회공학의 고전적인 예이다. 또 다른 예로는 친구로부터 온 편지를 가장하여 상대방의 컴퓨터를 바이러스에 감염시키는 멜리사 바이러스가 있다. 그 편지에 첨부된 바이러스를 인식하지 못하고 확인한 사용자나, 매크로 바이러스에 대한 대비책이 없는 사용자는 자기 자신의 컴퓨터뿐만 아니라 다른 사람에게도 바이러스를 전파시키게 된다. 사회 공학적 공격기법은 사람에 의해서도 행해질 수 있다. 따라서 보안 담당자는 알려지지 않은 사용자가 어떠한 정보에 접근을 시도하거나 갱신을 요구할 때, 그 사용자의 ID뿐만 아니라 부가적인 다른 정보를 요구하여야 한다.

IV. 보안도구 우회공격 대응방안

4.1 패킷 필터링에 의한 공격 대응방안

4.1.1 Insertion 우회공격기법 대응방안

Unicode를 이용한 Insertion 공격 대응방안은 URL encoding의 경우 IDS이 UTF8, HEXA, Percent, Double-eval encoding을 이용하여 변형된 부분을 일반적인 ASCII값으로 변경할 수 있는 능력을 갖춘다면 공격을 탐지할 수 있다. Long URLs의 경우 이 공격은 IDS이 가지는 탐지 알고리즘에 의존한다. 즉, 오용탐지 방식의 IDS이 가지는 단점을 이용한 것으로 적절한 방어와 탐지를 위해선 정상행위에 대한 프로파일을 만들어 이에 벗어나는 행위를 탐지하는 비정상행위 탐지 방식을 탐지 시스템이 지원하여야한다. Multiple slashes의 경우 IDS의 탐지 규칙에 "/cgi-bin/test.cgi"와 "//cgi-bin //test. test.cgi"를 모두 추가하거나, '//', '/'를 동일하게 인식하는 알고리즘을 사용하였을 때 공격을 탐지 할 수 있다. Reverse traversal의 경우 IDS의 탐지 규칙에 변경 가능한 모든 디렉토리의 경로를 추가할 경우 공격을 탐지 할 수 있다. Self-Referencing Directories IDS이 자기 자신의 디렉토리를 참조하는 './'문장을 발견했을 때 제거하는 알고리즘을 통하여 공격을 탐지 할 수 있다.

4.1.2 Evasion 우회공격기법 대응방안

공격자가 사용하는 Evasion 기법을 사용하는 우회공격은 IDS의 기본적인 탐지 알고리즘과 보안도구가 사용하는 네트워크 프로토콜의 문제점을 이용한 것이 대부분이다. 현재 판매되고 있는 침입탐지 시스템이 사용하고 있는 탐지 알고리즘은 거의 동일한 방법을 채택하고 있다. 단지 차이점은 어느 시스템이 더 많은 규칙 데이터 베이스를 가지고 있는 가의 여부이다. Unicode Bypass Vulnerability의 경우는 침입자가 탐지 룰 데이터 베이스를 분석함으로서 우회 방법을 연구할 수도 있다. Unicode Bypass 취약성의 경우는 비표준 Unicode 형식(%u 인코딩)을 검출하는 시그너처에 추가하거나, 변형시킬 수 있는 프로그램을 IDS내에 삽입함으로서 우회공격을 막을 수 있다. 이러한 침입을 방어하기 위해서는 IDS상의 탐지 시그너처를 최신으로 유지하도록 정의된 작업 과정을 가지고 있는 것이 매우 중요하다. 새로운 공격은 계속 개발되므로, IDS 플랫폼은 자주 갱신되어야 한다. 안티 바이러스 도구를 바이러스의 급속한 개발과 확산 때문에 호스트에서 최신으로 유지하는 것처럼, IDS 시스템을 최신으로 유지해야 한다. 웹, DNS 혹은 메일 서버와 같은 중요한 서버에 대해서는 호스트 기반 IDS를 설치한다.

Session splicing의 경우에는 OS에서의 세션 재조합 하는 시간에 따라 달라질 수 있다. 따라서 시그너처 구성시 해당하는 OS와 세션 시간의 매치를 넣어줌으로써 우회공격을 방어할 수 있다. 또한

IDS 모듈 구성시 세션 재조합 모듈 함수를 구성하여 비교할 수도 있다.

4.2 TCP/IP 특성에 의한 공격 대응방안

4.2.1 IP layer 우회공격기법 대응방안

가. IP Insertion 공격에 대응방안은 IDS가 탐지하는 패킷과 end-system에 수신되는 패킷이 일치되도록 해야 한다. 또한 IDS와 end-system의 패킷을 처리하는 방법이 일치되도록 해야한다. 그러므로, IDS는 네트워크 구조상의 위치가 중요하며, end-system들이 패킷을 처리하는 방법들을 모두 알고 있어야 한다. IDS와 end-system의 네트워크 위상이 차이 제거하거나, DF 옵션을 이용한 우회 기법의 경우, IDS 네트워크의 최대 패킷 사이즈(MTU)와 end-system 네트워크의 최대 패킷 사이즈를 같게 하여, DF 옵션과 패킷의 사이즈와 무관하게 IDS와 end-system이 수신할 수 있는 패킷을 일치시킬 수 있다. IDS와 end-system이 패킷을 처리하는 방법을 일치(IP 옵션) end-system이 IP 옵션(timestamp, checksum)을 조사하여 패킷의 허용 유무를 결정하는 방법과 같이 IDS에서도 수행되어야 한다. 즉, IDS가 각 end-system의 OS별 데이터(패킷)의 처리과정을 정확히 인식하여 패킷의 허용 유무를 end-system에서와 같이 결정하여야 한다. 예를들어, IDS는 수신한 패킷의 timestamp가 end-system 입장에서 유효한지 그리고 checksum이 일치하는지를 판단할 수 있어야 한다.

나. MAC Address의 경우 IDS가 수신 받은 패킷의 MAC 주소를 확인하거나 IDS가 올바른 link-layer 주소의 IP 헤더에 수신지 주소를 확인하여 공격자가 네트워크 모니터의 link-layer 주소를 알지 못하더라도, 패킷을 가짜 주소로 설정하여 네트워크 모니터가 오작동 하도록 할수 있다. 그러므로, IDS는 올바른 link-layer 주소 패킷이라도 IP 헤더의 수신지 주소를 확인하여, 주소가 잘못 설정된 link-layer 프레임으로 판단하지 않도록 해야 한다.

다. IP covert channel의 경우 IP 헤더 필드를 이용한 은닉채널 형성 기법과 IP 계층의 ICMP와 같은 프로토콜을 이용하는 은닉채널 형성 기법으로 분류되며 각각에 대한 대응방안 마련이 필요하다. 먼저 IP 헤더를 이용하는 은닉채널 형성 기법에 대한 대응방안은 먼저 수신한 IP 패킷의 헤더 필드 값들이 TCP/IP 규약에 벗어나는지를 검사하는 것이다. 하지만 대부분의 IP 헤더를 이용하는 은닉채널 형성 기법은 이런 규약을 벗어나지 않는다. 또한 IP 헤더의 특정 필드를 이용하는 공격 도구가 있다면 알려진 공격 도구에 대한 분석 후 대응방안을 마련하는 것도 하나의 방법이 될 수 있다. 하지만 이러한 특정 도구에 대한 대응방안은 향후 발생할 수 있는 여러 가지 변형 도구에 대한 공격에 취약할 수밖에 없다. 따라서 신경망 학습과 같은 비정상패턴에 대한 학습 기법의 사용이 요망된다. 두 번째로 IP 계층의 프로토콜을 이용하는 은닉채널 형성기법의 경우에는 마찬가지로 특정 도구에 대한 방지 룰을 만드는 것이 선행되어야겠지만, 향후에는 변형 기법에 대비한 신경망 기반의 비정상패턴 탐지 방안이 마련되어야 한다.

4.2.2 TCP layer 우회공격기법 대응방안

가. TCP Insertion의 경우 TCP 패킷의 데이터를 확인하기 전에 헤더 필드를 확인하거나 TCP 상황에 따른 SYN 패킷 데이터 판단, 연결 상태에 따라 TCP Option을 확인하여 연결의 상태에 따라 TCP 옵션에 대한 규정이 결정되므로, IDS도 연결 상태를 고려하여 TCP 옵션을 처리하여야 한다. 즉, TCP 옵션에 대한 판단 기준이 IDS와 end-system 간에 일치하여야 한다. 예를 들어, IDS는 수신 시스템이 PAWS를 제공하는지에 대해서 알아야할 뿐만 아니라, 수신 시스템의 time-stamp에 한계 값도 알아야만 한다.

나. TCP Reassembly의 경우 시퀀스 넘버를 사용하거나 IDS와 윈도우의 동기화, IDS와 시스템 간의 규칙일치 기법등이 존재한다.

다. TCP De-synchronization의 경우 IDS에서 부분적인 핸드쉐이크를 허가하거나 SYN 패킷들을 무시하여 IDS가 SYN 패킷은 무시하고, 데이터는 시퀀스 넘버를 초기화하는데 사용한다. SYN 패킷을 무시하므로 재동기화할 필요가 없다. 이것은 Post Connection Desynch를 완벽하게 막을 수 있으나, 공격에 의해 동기화가 되면 그 동기화를 해제할 수 있는 대안이 없다. SYN 패킷을 사용하는

IDS에서의 Desynch 대응방안은 잠정적으로 SYN 패킷을 사용하는 IDS에서의 Desynch를 해결하는 해결방안은 IDS에서 동기화하는 것을 허용은 하되, 때때로 시작할 때 기록해 놓았던 3WH 패킷들을 검사하는 것이다. 이 방법은 처음 관찰된 데이터로 연결을 초기화하고, 실제 3WH가 실행되는 것이 보이면 이 때 다시 연결을 초기화한다. 즉, 3WH는 실제 상태를 설정하는데 사용하고, 이전 상태와 기록된 데이터들은 조작된 것으로 간주한다. 이것은 Pre Connection Desynch에 대해서 취약할 수 있으므로 이것을 극복하기 위해 SYN+ACK 패킷을 사용한다. 공격자가 서버에서 오는 SYN+ACK 패킷을 위조할 수 없는 한(spoof-protection 필터링이 있다면, SYN+ACK 패킷을 위조하는 것은 거의 불가능하다) IDS는 서버로부터 오는 SYN+ACK 패킷을 실제 연결이 이루어지는 것이라고 신뢰할 수 있다.

마. TCP covert channel

보안도구들에 대한 우회공격기법 중 TCP 프로토콜 기반의 은닉채널을 형성하는 우회공격기법에 대한 대응방안은 IP 프로토콜 기반의 은닉채널 형성 우회공격기법 대응방안과 동일하다. 먼저 수신된 패킷이 TCP/IP 프로토콜 규약을 준수하는지를 검사해야 한다. 하지만 이런 규약을 준수하는 패킷에 대한 은닉 채널 형성 유무는 일반적인 스트링 패턴 룰 매칭으로 탐지하기 어렵다. 우선 TCP 기반의 은닉채널 형성 도구에 대한 분석 후 탐지룰을 만드는 것도 하나의 방법이 되겠지만, 수신된 은닉 채널 패킷의 헤더 값들이 정상적인 방법으로 생성된 것이기 때문에 패턴 매칭 기반의 룰 셋으로 판별하기가 어렵다. 따라서 정상적인 TCP/IP 헤더와 은닉채널 형성 우회공격 도구가 생성하는 비정상적 TCP/IP 헤더를 신경망 등의 학습 기법으로 판별하는 것과 같은 비정상행위 기반의 우회공격 탐지 기법이 필요하다.

4.3 보안도구 취약성에 공격 대응방안

현재 정보보호 솔루션의 대다수를 차지하고있는 IDS, Firewall, Router 등은 익명의 공격자로부터 데이터 및 시스템을 보호하고 있다. 하지만 관리자의 부주의, 보안도구의 잘못된 설정 그리고 보안도구의 취약성 때문에 공격을 당할 수 있다. 후자의 경우 해당 보안도구제품의 웹사이트를 통하거나 CD-ROM을 통하여 패치를 수행할 수 있다.

4.4 사회공학기법에 의한 공격 대응방안

사회공학을 이용한 공격은 기술적인 공격방법과는 달리 관리자의 세심한 주의를 필요로 한다. 앞에서 설명했듯이 위 공격방식은 일상생활에서 항상 일어날 수 있는 일을 가장하여 시스템을 해킹하는 방법이기 때문에 이러한 형태의 공격들을 시스템의 관리자나 회사 직원이 그들 주변에서 일어나는 일을 충분히 인식 할 수만 있다면 막을 수 있다. 이러한 방법으로는 훈련, 정책, 인식등의 방법이 존재 한다.

V. 우회공격 도구 분석

본 절에서는 우회공격 도구와 앞서 분석된 우회공격기법과의 상관관계에 대해서 분석하였다. 표 5-1은 3장의 우회공격기법 분류표를 참고하여 우회공격 도구의 우회공격기법을 분류하였다. fragrouter 도구의 경우에는 실제적인 우회공격을 수행하는 공격도구는 아니지만 패킷 필터링 기반의 evasion 공격 중 fragmentation과 TCP/IP 기반의 IP 계층에서의 IPfragmentation 기법을 수행한다. whisker는 패킷 필터링 기반의 insertion 공격기법 및 TCP/IP 각 계층에서의 insertion 공격기법 등을 수행한다.

CovertTCP와 Loki2의 경우에는 은닉채널을 형성하는 공격 도구인데, CovertTCP의 경우에는 IP 계층의 identification field, TCP 계층의 initial sequence number, acknowledge number 등을 이용한 은닉채널 형성에 사용되며, Loki2의 경우에는 ICMP 페이로드를 이용한 은닉채널 형성에 사용된다. 마지막으로 IDSWakeup, Snot, Sidestep의 도구는 종합적인 NIDS 우회공격 및 테스트 도구로서 IDSwakeup의 경우는 전형적인 false-positive 유발을 통한 NIDS 검증 도구이며, Snot의 경우는 snort의 룰 변형을 통한 기법을 사용하고, Sidestep의 경우 그 이름과 같이 보안도구의 어떤 부수적인 역효과를 발생시키는데 그 목적이 있는데 현재 프로그램 자체가 바이너리 코드로만 제공되기 때문에 그 자세한 분석에는 어려움이 있다. 다만 공격 도구 매뉴얼에 의해 evasion, false-positive등 다양한 우회공격을 시도한다.

〔표 2〕 우회공격 도구

우회공격 도구	대표적인 공격 특성	분류인덱스
fragrouter	패킷 필터링 기반의 evasion	FS-E-다
	IP fragmentation	TI-N-다
whisker	패킷 필터링 기반의 insertion	FS-I-가, FS-I-나
	TCP insertion	TI-T-가
	IP insertion	TI-N-가
CovertTCP	IP Covert Channel	TI-N-라
	TCP Covert Channel	TI-T-마
Loki2	IP Covert Channel	TI-N-라
Sidestep	패킷 필터링 기반의 insertion	FS-I-가, FS-I-나
	패킷 필터링 기반의 evasion	FS-E-가
	그 외 TCP/IP 공격들	-
IDSWakeup	패킷 필터링 기반의 insertion	FS-I-가, FS-I-나
	패킷 필터링 기반의 evasion	FS-E-가
	패킷 필터링 기반의 DoS	FS-D-가, FS-D-나
	TCP insertion	TI-T-가
	IP insertion	TI-N-가
Snot	패킷 필터링 기반의 insertion	FS-I-가, FS-I-나
	패킷 필터링 기반의 evasion	FS-E-가
	패킷 필터링 기반의 DoS	FS-D-가, FS-D-나
	TCP insertion	TI-T-가
	IP insertion	TI-N-가

Ⅵ. 결론 및 향후 연구 방향

본 논문에서는 국내·외의 보안도구 우회기법에 대한 동향 및 현황을 파악하였다. 현재 사용되는 대부분의 우회도구 공격기법들은 대부분이 IDS에 초점을 두고 있지만, IDS에 우회를 목적으로 하는 도구일지라도 사용되는 우회기법의 특성상 패킷 필터링에 기반 한 보안 도구인 경우에 IDS, Firewall 등의 구분은 큰 의미가 없다. 또한 TCP/IP 프로토콜의 터널링 특성을 이용한 Covert Channel 우회 기법은 어떤 보안도구를 사용할지라도 생성되는 Covert Channel의 특성을 파악하지 못한다면 우회공격에 대해 특별한 대응방안을 마련하기 어렵다.

그러므로 이러한 연구를 통해 보안도구에 따른 우회 기법의 연구보다는 현재보고 되고 있는 여러 보안 도구 우회기법들을 기법 자체의 특성에 따라 분류하여 각 기법에 대한 대응방안에 대하여 연구하는 것이 보다 바람직한 연구 방향이라 생각되어 다음과 같이 보안도구의 패킷 필터링 특성에 의한 우회공격 기법 분석, TCP/IP 특성에 의한 우회공격 분석, 보안도구 취약성에 의한 우회공격기법 분석, 사회 공학적 기법에 의한 우회공격기법 분석 등으로 구분하여 우회공격기법을 분석하고 그 대응방안을 제시하였다.

또한 이렇게 분류되어 연구된 우회 기법을 바탕으로 대표적으로 사용되는 다음의 fragrouter, whisker, CovertTCP, loki2, IDSwakeup, SideStep, Snot과 같은 우회공격 도구를 분석함으로써 실제적인 우회 기법의 위험성 및 그 탐지 대응책을 연구하였으며 공개용 IDS snort 룰을 이용한 탐지 룰셋을 작성의 기반을 마련하였다.

향후에는 보다 다양한 공격기법에 대한 탐지가 가능하며 탐지율을 높일 수 있는 우회공격기법 탐지 도구의 개발을 필요로 한다.

참 고 문 헌

〔1〕 Thomas H.Ptacek, Timothy N.Newsham "Inserti on, Evasion, and Denial of Service: Eluding Network Intrusion Detection", January 1998, http://citeseer.nj.nec.com/ptacek98insertion.html

〔2〕 Fred Cohen, 50 ways to defeat your intrusion Detection System http://all.net/

〔3〕 Coretez Giovanni, "Passive Mapping :Anoffensive use of IDS", http://www.eurocompton.net/stick/papers/OffensiveUseofIDS.pdf

〔4〕 Greg Hoglund, Jon Gary, "Multiple Levels of De-synchronization and other concerns with testing an IDS system". August, 2000. URL: http://online. securityfocus.

com/infocus/1204
[5] IDS Evasion Techniques and Tactics, Kevin Timm, May 7, 2002, http://online.securityfocus.com/infocus/1577
[6] IDS Evasion with Unicode, Eric Hacker, Jan. 3, 2001, http://online. securityfocus. com/infocus/1232
[7] Re-synchronizing a NIDS, Eric Hacker September 22, 2000, http://online.securityfocus.com/infocus/1226
[8] Social Engineering: Techniques that can bypass Intrusion Detection Systems, Toby Miller, June 19, 2000, http://online. securityfocus.com/infocus/1229
[9] T. Ptacek and T. Newsham, Secure Networks Insertion, Evasion, and Denial of Service:Eluding Network Intrusion Detection, January 1998., http://citeseer. nj.nec.com/ptacek98insertion.html
[10] Comer, D. E. [1995] Internetworking with TCP/IP Volume One, Prentice-Hall, Upper Saddle River, New Jersey
[11] route [1996] Phrack Magazine Issue 49 Article 6, Phrack Magazine,San Francisco, California
[12] Defeating Sniffers and Intrusion Detection Systems, horizon, Phrack Magazine, Volume 8, Issue 54, article 10 of 12, Dec 25th, 1998,
[13] Loki: ICMP Tunneling, daemon9, Pharack Magazine, Volume 6, Issue 49, article 6 of 16,
[14] LOKI2 (the implementation), route, Phrack Magazine, Volume 6, Issue 51, article 6 of 17,
[15] François-René Rideau, "Firewall Piercing mini-HOWTO", http://secinf.net /info/fw/fwp/Firewall-Piercing.html
[16] Van Hauser, "Placing Backdoors Throught Firewalls",http://www.securitymap.net/sdm/docs/attack/fw-backd.htm
[17] Steven Martin, "Anti-IDS Tools and Tactics", http://rr.sans.org/intrusion/anti-ids.php
[18] Defending Against NIDS Evasion using Traffic Normalizers, Vern Paxson, Mark Handley, ACIRI, RAID, Sept '99
[19] Solar Designer. Non-Executable User Stack. http://www.openwall.co/linux/.
[20] Chris Evans. Nasty security hole in lprm. Bugtraq mailing list, http://geek-girl.com/bugtraq/, April 19 1998.
[21] Nothan P. Smith. Stack Smashing vulnerabilities in the UNIX Operating System. http://millcomm.com/nate/machines/security/stack-smashing/nate-buffer.ps, 1997.
[22] Rafel Wojtczuk. Defeating Solar Designer Non-Executable Stack Patch. Bugtraq mailing list, http://geek-girl.com/ bugtraq/, January30 1998.
[23] TIS Committee, May, 1995, Tool Interface Standard(TIS) Executable and Linking Format(ELF) Specification V.1.2

〈著 者 紹 介〉

손 태 식 (Tae Shik Sohn)
학생회원

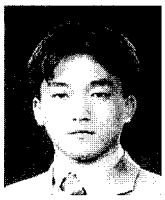
2000년 2월 : 아주대학교 정보 및 컴퓨터 공학부 졸업(공학사)
2002년 2월 : 아주대학교 정보통신전문대학원 정보통신공학과 졸업(공학석사)
2002년 3월~현재 : 고려대학교 정보보호대학원 박사과정
관심분야 : 네트워크·시스템보안, 인터넷프로토콜 보안

서 정 우 (Jung Woo Seo)

2002년 2월 : 호남대학교 정보통신공학부 졸업(공학사)
2002년 3월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 네트워크·시스템보안, 생체인식

구 원 본 (Won Bon Koo)

2002년 2월 : 고려대학교 공학부 졸업(공학사)
2002년 3월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 시스템 보안



민 동 옥 (Dong Ok Min)

2002년 2월 : 고려대학교 공학부 졸업(공학사)
2002년 3월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 시스템 보안

문 종 섭 (Jong Sub Moon) 정회원

1981년 2월 : 서울대학교 계산통계학과 학사
1983년 2월 : 서울대학교 계산통계학과 석사
1992년 2월 : Illinois Institute of Technology 박사
1993년 ~현재 : 고려대학교 전자 및 정보공학부 교수
고려대학교 정보보호대학원 겸임 교수
관심분야 : IDS, 신경망, 생체인식, 운영체제

박 현 미 (Hyun Mee Park)

1996년 2월 : 전북대학교 컴퓨터과학과 학사
1996년 2월~현재 : 한국정보보호진흥원 연구원
관심분야 : 정보보호

이 병 권 (Byung Kwon Lee)

1989년 2월 : 전북대학교 컴퓨터공학 학사
1992년 2월 : 포항공과대학교 전산학 석사
2001년 1월~현재 : 한국정보보호진흥원 선임연구원
관심분야 : 정보보호